CYBER LAB

Комплекс криптографічного захисту інформації "Криптосервер 2.0"

Загальні відомості

Комплекс криптографічного захисту інформації "Криптосервер 2.0" забезпечує криптографічний захист інформації з обмеженим доступом та відкритої інформації, вимога щодо захисту якої встановлено законом, та яка передається в IP-мережах загального користування.

Призначення

Комплекс криптографічного захисту інформації "Криптосервер 2.0" призначений для криптографічного захисту інформації, яка передається через незахищене середовище (мережею Internet, MPLS) шляхом створення захищених каналів передачі даних за технологією віртуальних приватних мереж типу IPsec.

Необхідність

Комплекс криптографічного захисту інформації "Криптосервер 2.0" застосовується для криптографічного захисту інформації, яка циркулює в автоматизованих системах класу 2 та класу 3, шляхом її шифрування та забезпечення цілісності при її передачі.

Вимога п.9 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, які затверджені Постановою КМУ від 29 березня 2006 № 373 (із змінами)

Компоненти комплексу

- ✓ "Серверний модуль" зі складу "Комплексу"
- ✓ "Клієнтський модуль" зі складу "Комплексу"
- ✓ "Центр генерації ключів" зі складу "Комплексу"
- ✓ "Модуль керування" зі складу "Комплексу"
- ✓ "Модуль моніторингу" зі складу "Комплексу"
- ✓ "Конфігураційний модуль" зі складу "Комплексу "

Криптографічні алгоритми

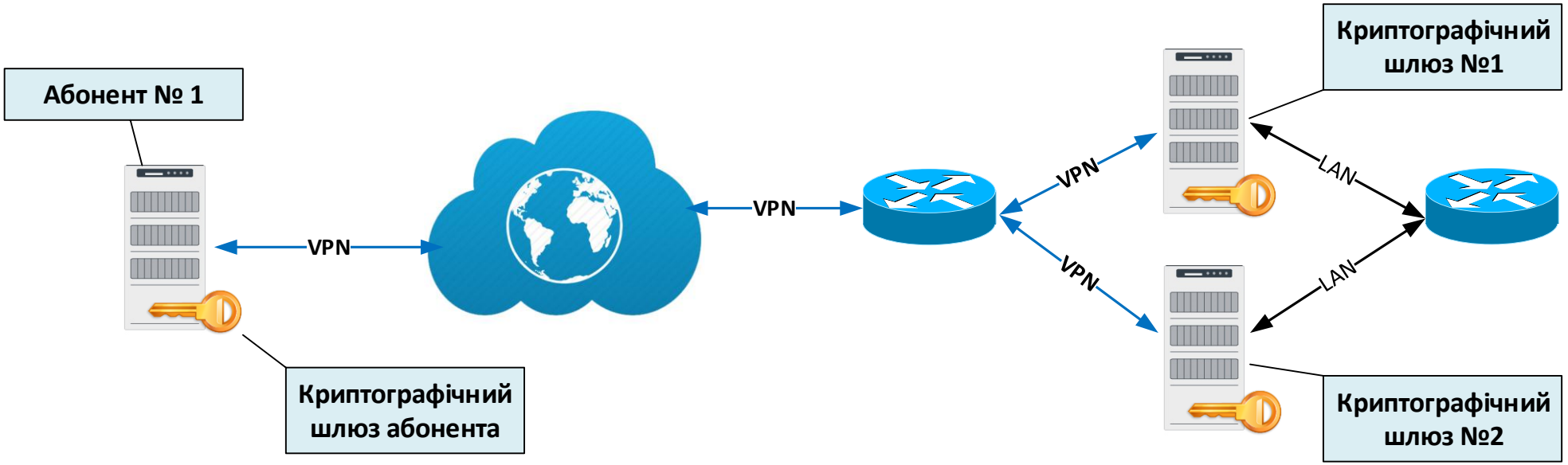
- ✓ шифрування даних відповідно до ДСТУ 7624:2014 - "Калина";
- ✓ електронний підпис відповідно до ДСТУ 4145-2002;
- ✓ гешування відповідно до ДСТУ 7564:2014 - "Купина";
- ✓ протокол розподілу ключових даних відповідно ДСТУ ISO/IEC 15946-3:2015.

Криптографічні алгоритми

- ✓ шифрування даних відповідно до ДСТУ ISO/IEC 18033-3:2015 - "AES" ;
- ✓ електронний підпис відповідно до IETF RFC 8017 - "RSA";
- ✓ гешування відповідно до ДСТУ 10118-3:2005 - "SHA-1, SHA-256, SHA-512";
- ✓ протокол розподілу ключових даних відповідно ДСТУ ISO/IEC 15946-3:2015.

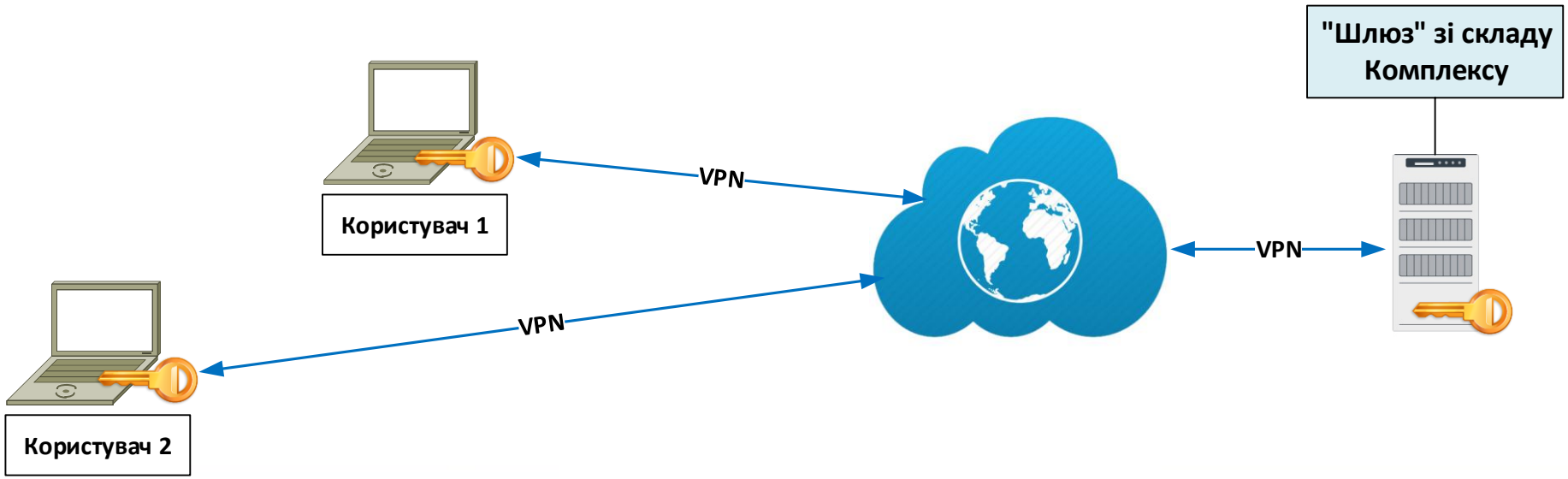
Приклади використання

- ✓ "Мережа-Мережа" (Сервер-Сервер) - утворення захищених каналів передачі даних між різними розподіленими мережами із забезпеченням захисту всього трафіку передачі;



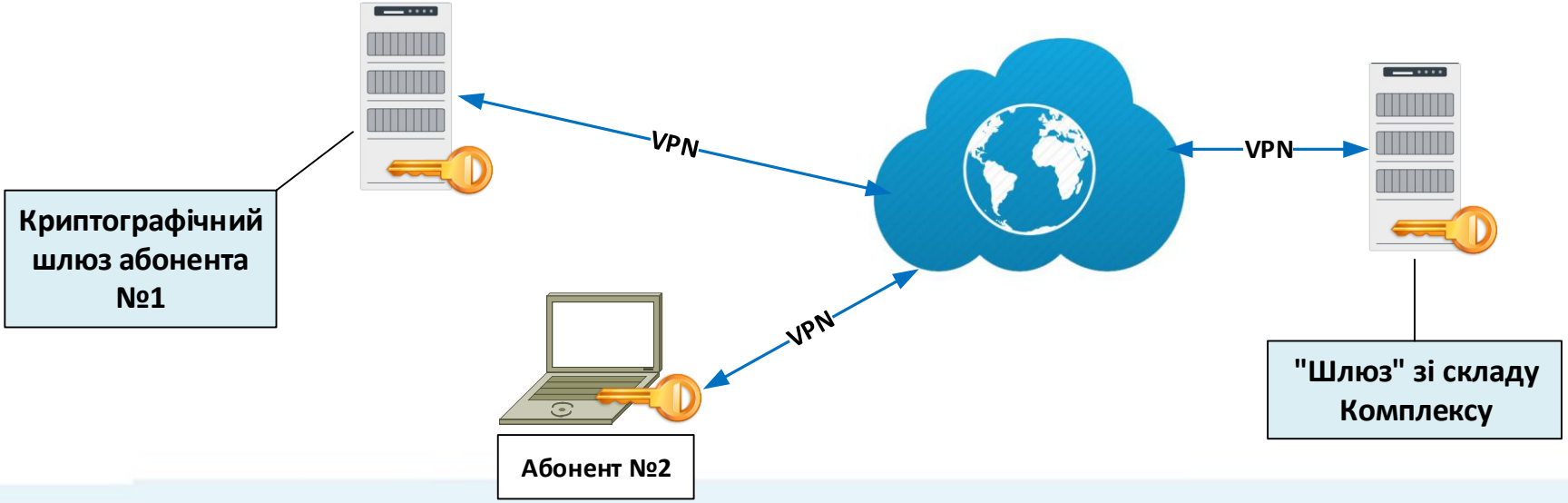
Приклади використання

- ✓ "Користувач-Мережа" (Клієнт-Сервер) - утворення захищених каналів передачі даних між комп'ютером користувача та комп'ютерною мережею, яка розміщена за модулем "Шлюз".



Приклади використання

- ✓ "Гібридна мережа" (Сервер-Сервер-Клієнт) – утворення захищених каналів передачі даних між різними розподіленими мережами, а також між комп'ютером користувача та комп'ютерними мережами, які розміщені за модулем "Шлюз".



Переваги

- ✓ Прозорість проходження захищеного мережевого трафіку для Firewall, Proxy, Network Address Translation.
- ✓ Зручне налаштування модулів "Шлюз" та "Клієнт" шляхом запису конфігурації мережі у файли налаштувань.
- ✓ Можливість моніторингу стану захищених каналів передачі даних з використанням агентів та розширень системи моніторингу мереж Zabbix.

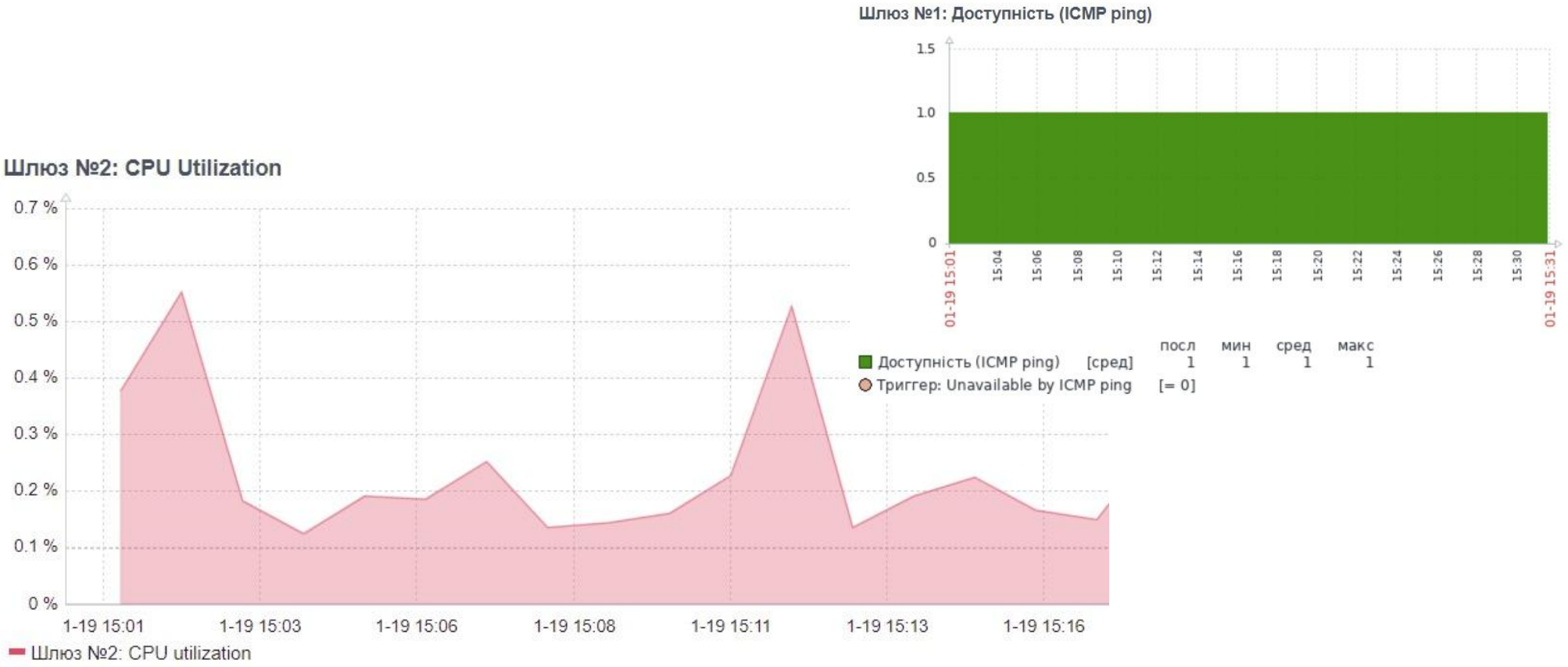
ZABBIX

Моніторинг

- ✓ доступності захищеного каналу зв’язку;
- ✓ значення часу відповіді в захищеному каналі зв’язку;
- ✓ наявності проблем в захищеному каналі зв’язку;
- ✓ статусу функціонування сервісу «шифрування»;
- ✓ рівня використання мережевих інтерфейсів, вільного місце на жорсткому диску, значень використання центрального процесору та пам’яті;
- ✓ інших параметрів.

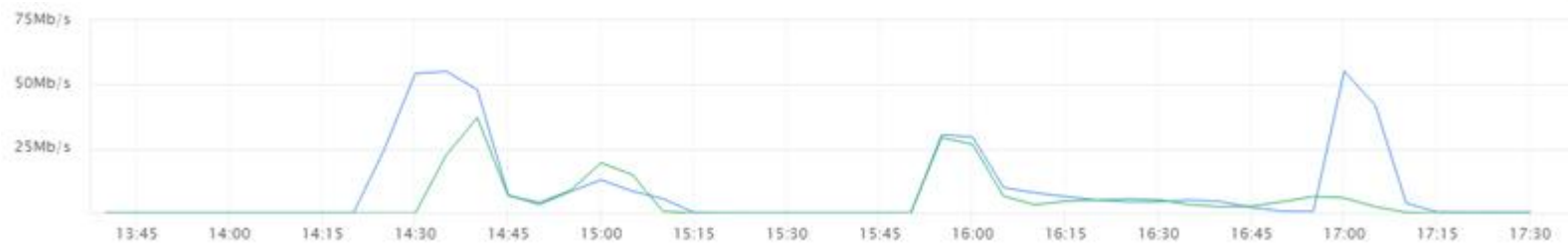
Узел сети	Имя ▲	Последняя проверка	Последнее значение
Шлюз №1	Доступність	15.12.2021 15:54:11	Down (0)
Шлюз №1	Мережеві проблеми	15.12.2021 15:54:11	100 %
Шлюз №1	Час затримки	15.12.2021 15:54:11	0

Приклади моніторингу



Переваги

- ✓ Балансування захищеного мережевого трафіку шляхом логічного поєднання декількох модулів "Шлюз".
- ✓ Збільшення пропускної здатності захищеного мережевого трафіку за рахунок агрегації мережевих інтерфейсів.
- ✓ Реалізація механізмів відмовостійкості роботи модулів "Шлюз" за рахунок використання відповідних мережевих протоколів.



Особливості застосування

- ✓ зручність управління ключовими даними та конфігураціями комп’ютерних мереж;
- ✓ простота експлуатації та інтеграції в існуючу інфраструктуру інформаційно-комунікаційних систем;
- ✓ висока швидкість криптографічних перетворень, передачі даних та орієнтація на хмарні технології;
- ✓ широкий спектр підтримуваних апаратних та віртуальних платформ.

Віртуальні платформи.

- ✓ VMware;
- ✓ Microsoft Hyper-V;
- ✓ Nutanix Enterprise Cloud;
- ✓ Kernel-based Virtual Machine;
- ✓ Citrix XenServer;
- ✓ Oracle VM Server;
- ✓ Amazon Web Services
- ✓ Microsoft® Azure.

Підтримка Microsoft Azure

CRYPTOSERVER

Microsoft Azure

КОМПЛЕКС ПРОГРАМНИЙ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ "КРИПТОСЕРВЕР 2.0"

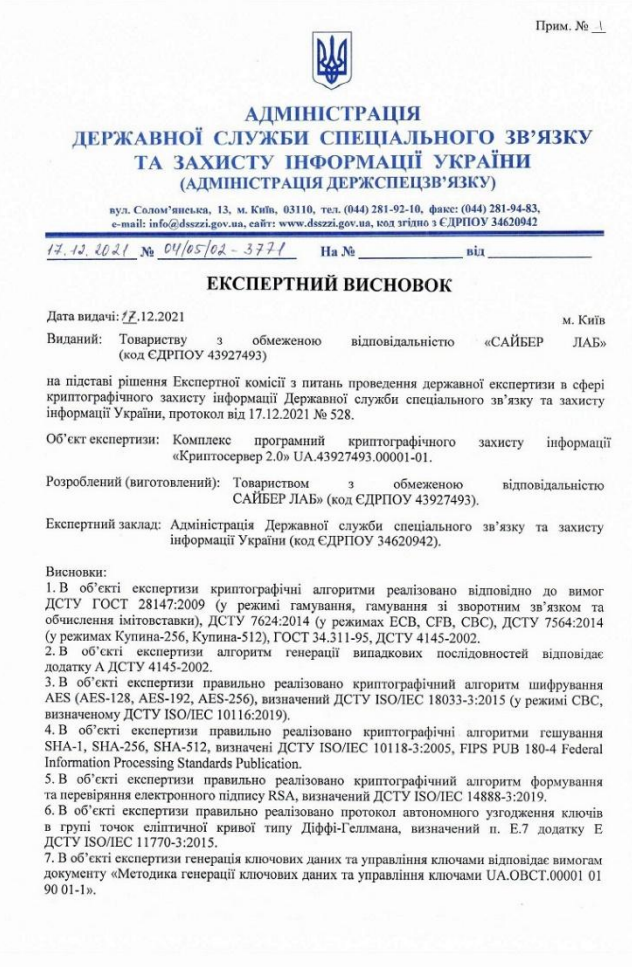
Підтримка Amazon

Державна експертиза

Комплекс програмний криптографічного захисту інформації "Криптосервер 2.0" відповідає Вимогам до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону, які затверджені наказом Адміністрації Держспецзв'язку від 07.05.2021 року № 278, що підтверджено за результатом державної експертизи.

Експертиза КЗІ

Комплекс програмний криптографічного захисту інформації "Криптосервер 2.0" має експертний висновок Адміністрації Держспецзв’язку за результатом державної експертизи в сфері криптографічного захисту інформації №04/05/02-3771 від 17.12.2021 р.



Прим. № 1

АДМІНІСТРАЦІЯ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ’ЯЗКУ)

вул. Солом’янська, 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

17.12.2021 № 04/05/02-3771 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 17.12.2021 м. Київ

Виданий: Товариству з обмеженою відповідальністю «САЙБЕР ЛАБ» (код ЄДРПОУ 43927493)

на підставі рішення Експертної комісії з питань проведення державної експертизи в сфері криптографічного захисту інформації Державної служби спеціального зв’язку та захисту інформації України, протокол від 17.12.2021 № 528.

Об’єкт експертизи: Комплекс програмний криптографічного захисту інформації «Криптосервер 2.0» UA.43927493.00001-01.

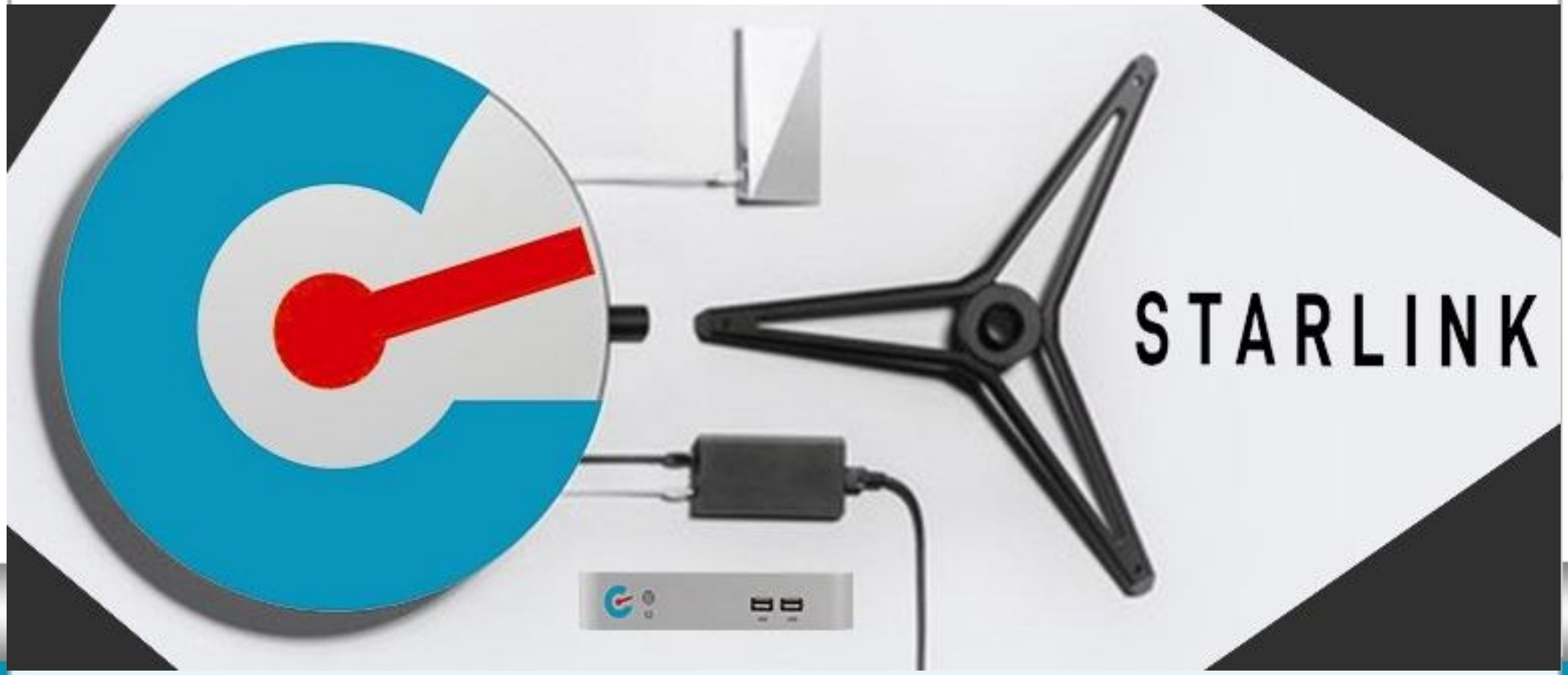
Розроблений (виготовлений): Товариством з обмеженою відповідальністю САЙБЕР ЛАБ» (код ЄДРПОУ 43927493).

Експертний заклад: Адміністрація Державної служби спеціального зв’язку та захисту інформації України (код ЄДРПОУ 34620942).

Висновки:
1. В об’єкті експертизи криптографічні алгоритми реалізовано відповідно до вимог ДСТУ ГОСТ 28147:2009 (у режимі гамування, гамування зі зворотним зв’язком та обчислення імітовставки), ДСТУ 7624:2014 (у режимах ECB, CFB, CBC), ДСТУ 7564:2014 (у режимах Купина-256, Купина-512), ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об’єкті експертизи алгоритм генерації випадкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об’єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES (AES-128, AES-192, AES-256), визначений ДСТУ ISO/IEC 18033-3:2015 (у режимі CBC, визначеному ДСТУ ISO/IEC 10116:2019).
4. В об’єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005, FIPS PUB 180-4 Federal Information Processing Standards Publication.
5. В об’єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-3:2019.
6. В об’єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана, визначений п. Е.7 додатку Е ДСТУ ISO/IEC 11770-3:2015.
7. В об’єкті експертизи генерація ключових даних та управління ключами відповідає вимогам документу «Методика генерації ключових даних та управління ключами UA.OBCT.00001 01 90 01-1».

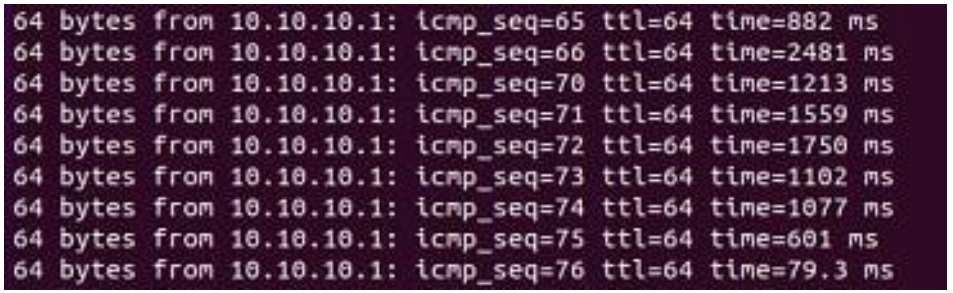
КОМПЛЕКС КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ "КРИПТОСЕРВЕР 2.0"

Шифрування STARLINK



Особливості функціонування

- ✓ обмін захищеним мережевим трафіком із використанням алгоритму шифрування "Калина" (ДСТУ 7624:2014);
- ✓ стабільний канал захищеного зв'язку при мережевих затримках "супутника";
- ✓ висока швидкість передачі даних захищеними каналами зв'язку навіть при значних завадах у "супутниковому" сигналі.



Технологічний стек

- ✓ мова програмування C та C++;
- ✓ фреймворк Qt;
- ✓ скрипти;
- ✓ IP Security відповідно до Request for Comments.

Контакти

Повна назва:
ТОВ "САЙБЕР ЛАБ"
support@c-lab.net.ua
https://c-lab.net.ua

Ми постійно працюємо над розширенням партнерської мережі, якщо Ви хочете стати нашим партнером напишіть нам про це: partner@c-lab.net.ua